AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
A black Samsung Galaxy J3 Emerge phone with the following identifiers: SM J327P; and IMSI: 310120233777159; and a white Sony Vaio Model PCG-3E2L laptop with the following identifiers: Service Tag: C1033Q0V; FCC ID: 2DS-BRCM1026; and IC: 9324A-BRCM1026 as more fully described in attachment A.

Case No. 5:18-MJ- 768 (DEP)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
A black Samsung Galaxy J3 Emerge phone with the following identifiers: SM J327P; and IMSI: 310120233777159; and a white Sony Vaio Model PCG-3E2L laptop with the following identifiers: Service Tag: C1033Q0V; FCC ID: 2DS-BRCM1026; and IC: 9324A-BRCM1026 as more fully described in attachment A.

located in the Northern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:
See attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC § 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:
See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Martin Baranski
Applicant's signature

Martin Baranski, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: December 21, 2018

David E. Peebles
Judge's signature

City and state: Syracuse, New York

Hon. David E. Peebles, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A
Property to Be Searched

This warrant applies to the following electronic devices seized from Kenneth Houck on December 11, 2018, and currently in the possession of law enforcement:

- A black Samsung Galaxy J3 Emerge phone with the following identifiers: SM J327P; and IMSI: 310120233777159; and
- A white Sony Vaio Model PCG-3E2L laptop with the following identifiers: Service Tag: C1033Q0V; FCC ID: 2DS-BRCM1026; and IC: 9324A-BRCM1026.

ATTACHMENT B

Particular Things to Be Seized

A complete forensic copy/mirror image of each electronic device described in Attachment A, as well as all information that constitutes fruits, contraband, evidence and instrumentalities of violation of 18 USC § 2252A, including information pertaining to the following matters:

a. The solicitation and coordination of activities associated with child pornography;

b. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;

c. Connection logs and records of user activity;

d. Records relating to SUBJECT ACCOUNT to include, but not limited to, correspondence, billing records, and any other subscriber information;

e. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

f. The identity of the person(s) who created or used the user IDs, including records that help reveal the whereabouts of such person(s);

g. The identity of the person(s) who communicated with the account about matters relating to the production, distribution, possession, and receipt of child pornography, including records that help reveal their whereabouts;

h. Any and all image and video files depicting any minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2); and

i. Any and all correspondence, chats, or other writings or documentation relating to the creation or production of sexually explicit images or videos of any minor, and

the transportation, distribution, receipt, possession, and access with intent to view said depictions.

I. Method of delivery

Governmetn-approved persons shall disclose responsive data if any, by sending said response to FBI Special Agent Martin Baranski, 250 South Clinton Street, Suite 330, Syracuse, NY 13202, by using the U.S. Postal Service or another courier service, notwithstanding the provisions of 18 U.S.C. § 2252A or any other law or regulation.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Martin Baranski, having been duly sworn, depose and state the following:

I. INTRODUCTION

1. I am a Special Agent employed by the United States Department of Justice, Federal Bureau of Investigation (FBI), and as such I am an "investigative or law enforcement officer" of the United States who is empowered by law to conduct investigations and to make arrests for offenses enumerated in Title 18, United States Code, Chapter 63. I have been a Special Agent with the FBI since October of 2018. I am currently assigned to the FBI's Albany Division where I investigate all federal criminal violations. I have participated investigations of persons suspected of violating federal child pornography laws, including Title 18, United States Code, Sections 2251, 2252 and 2252A. I have received training in the area of child sexual exploitation and have had the opportunity to observe and review examples of child pornography in all forms of media including computer media.

2. I make this affidavit in support of an application for a search warrant for information associated with an account that is stored at premises owned, maintained, controlled, or operated by GOOGLE, INC. (hereinafter Google), a provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The web-based electronic account service provided by Google, (hereinafter "account") including internet electronic mail (e-mail) to be searched is associated with email address with "donjuan6856833@gmail.com" and "kevinhogan9089@gmail.com," (hereinafter "SUBJECT ACCOUNT"), where your affiant believes exists evidence of criminal violations relating to violations of Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography), as more fully described in Attachment B.

3. The statements contained in this affidavit are based upon my investigation, information provided by other law enforcement officers, other personnel specially trained in the seizure and analysis of electronic media, and on my experience and training. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of a violation of 18 U.S.C. § 2252A exists in the accounts to be searched.

II. BACKGROUND CONCERNING GOOGLE, INC., GMAIL, AND GOOGLE DRIVE

4. The SUBJECT ACCOUNT is an internet account hosted by Google, Inc. (hereinafter, the "email provider"). In my training and experience, I have learned that Google provides a variety of online services, including email access, to the general public, allowing subscribers to obtain email accounts at the domain name *gmail.com*, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, Google servers are likely to contain stored electronic communications (including retrieved and unretrieved email for its subscribers) and information concerning subscribers and their use of Google's services, such as account access information, email transaction information, and account application information. Based on my training and experience and what I have learned from other law enforcement officers, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

5. In general, an email sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on the servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google servers for a certain period of time.

6. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to the servers, and then transmitted to its end destination. Email providers, like Google, often save a copy of the email sent. Unless the sender of the email specifically deletes the email from the email provider's server, the email can remain on the provider's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the provider's servers for a certain period of time.

7. A sent or received email typically includes at least the content of the message, source and destination addresses, the date and time at which the email or chat[1] was sent, and the size and length of the email or chat. If an email user writes a draft message but does not send it, that message may also be saved by the email provider but may not include all of these categories of data.

8. A Google subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, videos, and other files, on servers maintained and/or owned by Google. Gmail offers 15 gigabytes of free storage for messages and attachments. Additionally, Google offers optional paid plans for users to purchase extra storage in the following increments: 100 gigabytes; 1 terabyte; 2 terabytes; 10 terabytes; 20 terabytes; and 30 terabytes. Google offers a number of features to Gmail subscribers, including the ability to access Gmail from a cell phone, and a chat function allowing subscribers to send and receive instant messages and to save chat transcripts. In addition, users may archive Gmail in an "All Mail" archive. Archived mail can be stored and retrieved years later. Google also offers a feature allowing a subscriber to forward his Gmail to another e-mail account.

---

[1] Chat message is a common reference to instant message or a message sent via the Internet that appears on the recipient's screen as soon as it is transmitted.

9. Google+ (pronounced "Google Plus") Photos (formerly known as Picasa) is a photo and video storage and sharing service offered by Google. It allows Google account holders to store and share photos and videos with other users. In 2013, Google integrated Picasa Web Albums into Google+.

10. Google Drive is a file storage and synchronization service developed by Google. Google Drive allows users to store files in the cloud, synchronize files across devices, and share files. In addition to a website, Google Drive offers applications (apps) with offline capabilities for Windows and macOS computers, and Android and iOS smartphones and tablets. Google Drive is an office suite that permits collaborative editing of documents, spreadsheets, presentations, drawings, forms, and more, and encompasses Google Docs, Sheets, and Slides. Files created and edited through the office suite are saved in Google Drive. Users can upload files up to five terabytes in size. Users can change privacy settings for individual files and folders, enabling sharing with other users or making content public. The website and Android app offer a Backups section to see what Android devices have data backed up to the service.

11. Google subscribers can store emails, files, photos, and videos on Google+ and/or Google Drive. Doing so allows subscribers to access their data from any Internet-capable device, and enables them to store data remotely, rather than on their computers or personal electronic devices. In my experience and based on what I have learned as part of my job responsibilities from other law enforcement officers, subscribers of the email provider do not routinely keep their own copies of emails on home computers or other locations, although it is possible to do so, since their emails and other files stored on Google systems can be accessed readily from any internet capable device.

12. In my training and experience, email providers like Google generally ask each of their subscribers to provide certain personal identifying information when registering for an email account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Even if subscribers insert false information to conceal their identity this information often provides clues to their identity, location, or illicit activities.

13. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the email provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

14. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications,

including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. Such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

15. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. For example, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. Thus, email communications, chat communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. As described below, email providers typically log the IP addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Finally, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email

account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

III. THE INVESTIGATION AND FACTUAL BASIS

16. On February 23, 2012, Kenneth Houck pled guilty in the United States District Court for the District of Delaware to one count of transportation of child pornography in violation of Title 18, United States Code, Section 2252A(a)(1), and he was sentenced to an 87 month term of imprisonment.

17. Houck was released to a Residential Re-entry Center ("RRC") in August 2017, but he was sent back to prison after violating RRC rules. In July 2018, Houck was released from prison again, and on October 1, 2018, jurisdiction over Houck's supervised release was transferred to the Northern District of New York on October 1, 2018. Houck was homeless upon his release from prison, so the Court ordered him to reside in an RRC facility for three months. Houck was released from the RRC on November 30, 2018, and he moved to a residence in Syracuse, New York.

18. Houck's standard conditions of supervised release permit a probation officer to visit him at home or elsewhere and permit confiscation of any contraband observed in plain view of the probation officer. The special conditions of supervised release prohibit Houck from owning or operating in his home or any other location, including any place of employment, a personal computer or any electronic devices with internet access.

19. On December 11, 2018, Probation Officer Timothy Nolan, accompanied by a colleague, visited Houck's residence at Circle of Hope Residential Care, 2500 South Salina Street, Syracuse, New York, to conduct an inspection in order to determine Houck's adherence to the standard and special conditions of his supervised release. Another resident told the Probation Officers that Houck was upstairs in his bedroom. The Probation Officers approached the bedroom

and knocked several times, but nobody answered. Believing that Houck was nevertheless in the room, they opened the door to check on him. Houck was not in the room, but a black cellular telephone was plainly visible on a night stand next to the bed. After exiting the room, Probation Officer Nolan called Houck by cellular telephone, and Houck advised that he would be home soon. Upon Houck's arrival, he led the Probation Officers into his room, and Houck quickly moved to the night stand and appeared to put something in a pocket of his coat, which Houck then put on the bed. Probation Officer Nolan asked what was in the coat, and Houck denied that anything was in the coat. Houck eventually picked up the coat, and the same black cellular telephone was on the bed underneath where the coat had been. Houck denied having any other internet capable devices, but Probation Officer Nolan questioned him about this, in part because he noticed multiple charging devices in the room. Houck eventually admitted that he possessed a laptop computer as well, which Houck retrieved from a bin underneath his bed. After additional questioning, Houck admitted that he had been watching pornography on the devices—the laptop and cellular telephone.

20. Officer Nolan confiscated the laptop and the cellular telephone as contraband, as Houck's possession of them was a violation of his special conditions of supervised release. The phone seized from Houck (hereinafter, the "Samsung phone") was a Samsung Galaxy J3 Emerge phone with the following identifiers: SM J327P; and IMSI: 310120233777159. The laptop seized from Houck (hereinafter, the "Sony laptop") was a white Sony Vaio Model PCG-3E2L laptop with the following identifiers: Service Tag: C1033Q0V; FCC ID: 2DS-BRCM1026; and IC: 9324A-BRCM1026.

21. On December 12, 2018, Officer Nolan submitted an affidavit to Senior U.S. District Judge Norman A. Mordue of the Northern District of New York seeking authorization to search

the Samsung phone and the Sony laptop seized from Houck the day before. Judge Mordue granted the requested authorization,[2] after which Senior Probation Officer Scott Shanahan conducted a data extraction and forensic preview of both the Samsung phone and the Sony laptop. Upon the forensic preview, Officer Shanahan observed file names and paths indicative of potential child pornography in Google+ Photos and Google Drive accounts associated with "donjuan6856833@gmail.com" and "kevinhogan9089@gmail.com" accessible by the devices. The following file paths and names were observed by Officer Shanahan and are representative examples of the types of concerning file names and paths he observed:

a. Name: Fucking My Little Brother.MP4
Path: Google Drive Files donjuan6856833@gmail.com/Shared With Me/My Drive/My shit/Gay Incest Videos/Randoms/Fucking My Little Brother.MP4

b. Name: [KO kuruu] Young Boy Victim Of His Father - Incest.mp4
Path: Google Photos donjuan6856833@gmail.com/local media/[KO kuruu] Young Boy Victim Of His Father - Incest.mp4.mp4

c. Name: 2 brothers get in on.mp4
Path: Google Drive Files donjuan6856833@gmail.com/Shared With Me/My Drive/My shit/2 brothers get in on.mp4

d. Name: Dad and Son.MP4
Path: Google Drive Files donjuan6856833@gmail.com/Shared With Me/My Drive/My shit/Gay Incest Videos/Randoms/Dad and Son.MP4

22. These file names and paths are indicative of child pornography, as the names of the files likely describe the content of the files.

23. Based on my training and experience and what I have learned during the course of my investigation, including what I have learned about Houck's history of possession of child pornography, I respectfully submit there is probable cause to believe that these and potentially

[2] I have not received a copy of the affidavit or authorization, but I understand these facts to be accurate based on information learned from others during the course of my investigation.

other files in the SUBJECT ACCOUNT described further in Attachment A contain child pornography.

IV. ELECTRONIC STORAGE AND FORENSIC ANALYSIS

24. Based on my knowledge, training, and experience, I know that electronic devices such as the Samsung phone and the Sony laptop can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device that accessed the Internet. This information can sometimes be recovered with forensics tools.

25. *Forensic evidence.* This application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Samsung phone and Sony laptop were used, the purpose of their uses, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Samsung phone and/or Sony laptop because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

26. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Samsung phone and the Sony laptop consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of each entire device, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

27. *Manner of execution.* Because this warrant seeks only permission to examine electronic devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto premises. Consequently, I submit there is good cause for the Court to authorize execution of the warrant at any time in the day or night, as the forensic analysis and review will be undertaken by government-authorized persons according to their schedules. This warrant also authorizes the FBI to take possession of the electronic devices from any other law enforcement agency currently in possession of them in order to perform the needed extraction/analysis of them and to retain them as evidence of a crime and/or return them to the other law enforcement agency for safekeeping as evidence, as deemed prudent by government authorized persons.

V. CONCLUSION

28. Based upon the above information, I believe that Kenneth Houck has violated Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography), and that there is probable cause to believe that evidence of those crimes, more particularly described in Attachment B, exists and may be found on the Samsung phone and the Sony laptop, and I therefore

respectfully request that this Court issue a search warrant for these electronic devices, which are more fully described in Attachment A.

29. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that—has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

30. Upon executing the warrant and retrieving/extracting information from the Samsung phone and Sony laptop, government-authorized persons will review that information to locate and seize the items described in Attachment B. Notably, the government will retain a complete copy of the information retrieved/extracted from the devices for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

31. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

32. Finally, this Court has the authority to order government-approved persons to disclose responsive data to the Court's search warrant by sending it to the FBI Special Agent Martin Baranski using the U.S. Postal Service or another courier service, notwithstanding 18 U.S.C. § 2252A, or similar statute or code. Accordingly, Attachment B allows for sending results of the warrant and forensic analysis to your affiant by U.S. Mail or other courier.

Martin Baranski
Special Agent
Federal Bureau of Investigation

Sworn and subscribed to before me
this 18th day of December, 2018.

Hon. David E. Peebles
United States Magistrate Judge